CS 2050 Discrete Mathematics February 27th 2024

Lecture 14: Chinese Remainder Theorem

Lecturer: Abrahim Ladha

Theorem 1 (Chinese Remainder Theorem)**.** Given a set of linear congruences

$$\begin{aligned} x &\equiv r_1 \pmod{n_1} \\ x &\equiv r_2 \pmod{n_2} \\ &\dots \\ x &\equiv r_k \pmod{n_k} \end{aligned}$$

The number x has a unique value $\pmod{n_1 \cdot ... \cdot n_k}$ if and only if the numbers $n_1, ..., n_k$ are all pairwise relatively prime.

Proof. We will only do so informally. Let us suppose we have two equations.

$$\begin{aligned} x &\equiv a \pmod{n} \\ x &\equiv b \pmod{m} \end{aligned}$$

such that $\gcd(m, n) = 1$. We argue that a solution to x must exist (loosely), then more rigorously argue that such a solution is unique $\pmod{nm}$

□

We show a solution for x exists to simultaneously satisfy $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ with the assumption m, n are relatively prime.

We may write $x = a + my$ and $x = b + nz$ for some numbers z, y so

$$\begin{aligned} a + my &= b + nz \\ a + my &= b \pmod{n} \\ my &= b - a \pmod{n} \end{aligned}$$

since $\gcd(m, n) = 1$ then m^{-1} exists $\pmod{n}$. Lets call it m'. then

$$\begin{aligned} m'my &\equiv m'(b - a) \pmod{n} \\ y &\equiv m'(b - a) \pmod{n} \\ y &= m'(b - a) + nz' \end{aligned}$$

substitute this into $x = a + my$ to get

$$x = a + my = a + m(m'(b-a) + nz') = a + mm'(b-a) + mnz'$$

.

If we take this formulation of x and mod by m, n respectively we see that

$$\begin{aligned} x &\equiv a \pmod{n} \\ x &\equiv b \pmod{m} \end{aligned}$$

so such a solution to x has this form.

Next we prove that the solution is unique. Suppose that two distinct solutions exist (mod mn). There is a c, c' such that if $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ then $x \equiv c \pmod{mn}$ and $x \equiv c' \pmod{mn}$

Since $x \equiv a \pmod{m}$ then $c' \equiv c \pmod{m}$ and $c' \equiv c \pmod{n}$. So $m \mid c - c'$ and $n \mid c - c'$. Since m, n are relatively prime, then $mn \mid c - c'$. So $c \equiv c' \pmod{mn}$ and the solutions are not distinct.

1 An Example

There are a few ways to solve for x, I will demonstrate my favorite technique.

- $x \equiv 2 \pmod{3}$
- $x \equiv 3 \pmod{5}$
- $x \equiv 2 \pmod{7}$

First check that all the moduli are pairwise coprime. Here they are all prime so that follows immediately.

Take the last equation with the largest modulus, and rewrite it unmodular, so $x = 7k+2$ for some k. Then plug it into the second to last modulus to determine the residue of k.

$$\begin{aligned} 7k + 2 &\equiv 3 \pmod{5} \\ 2k &\equiv 1 \pmod{5} \\ k &\equiv 3 \pmod{5} \end{aligned}$$

So we know that $k = 5l + 3$ for some number l. Let us plug this back into x to get it in terms of l and not k to get

$$x = 7k + 2 = 7(5l + 3) + 2 = 35l + 23$$

Now take this form of x and put it into the last remaining equation

$$\begin{aligned} 35l + 23 &\equiv 2 \pmod 3 \\ 2l + 2 &\equiv 2 \pmod 3 \\ 2l &\equiv 0 \pmod 3 \\ l &\equiv 0 \pmod 3 \end{aligned}$$

So $l = 3r + 0$ for some number r. Then we plug this into x to get our final answer.

$$x = 35l + 23 = 35(3r) + 23 = 105r + 23$$

$$x \equiv 23 \pmod{3 \cdot 5 \cdot 7}$$

Our final answer is then $x = 23$.